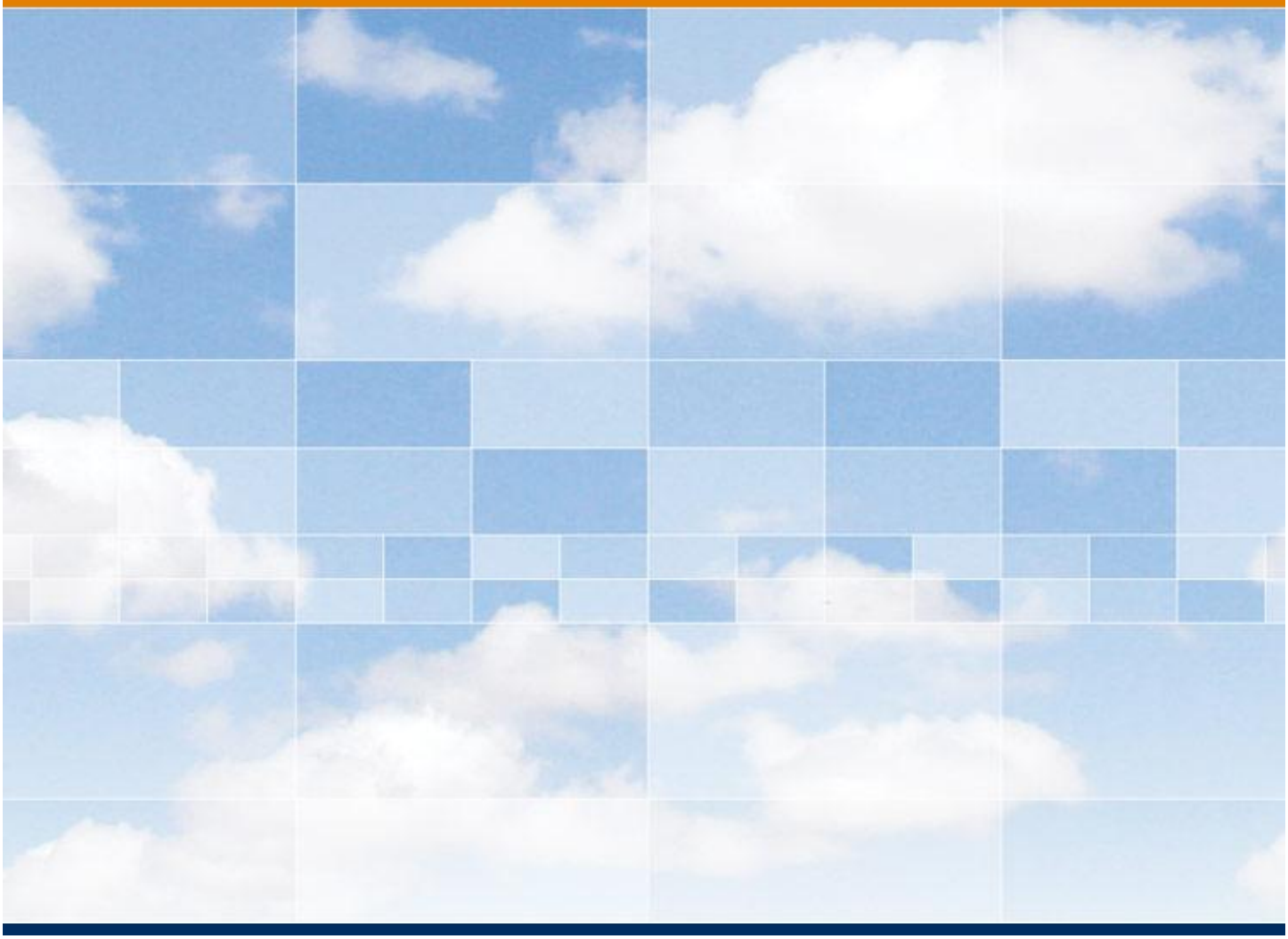
MatrikonOPC



Microsoft Windows DCOM Configuration

Windows XP SP3 and Server 2003 SP2 Configuration Guide

Microsoft Windows DCOM Configuration
Windows XP SP3 and Server 2003 SP2 Configuration Guide

This manual is a product of Matrikon Inc.

Matrikon Inc.
Suite 1800, 10405 Jasper Avenue
Edmonton, AB T5J 3N4
Canada

Phone: 780.448.1010
Fax: 780.448.9191
www.matrikonopc.com

Document Revision History:

Date	Document Version	Description	Author
2010-05-31	1.0	Converted to new template.	LB

SOFTWARE VERSION

Version: N/A

DOCUMENT VERSION

Version: 4.0

COPYRIGHT INFORMATION

CONFIDENTIAL

The information contained herein is confidential and proprietary to Matrikon Inc. It may not be disclosed or transferred, directly or indirectly, to any third party without the explicit written permission of Matrikon Inc.

LIMITATIONS

Matrikon has made its best effort to prepare this manual. Matrikon makes no representation or warranties of any kind with regard to the completeness or accuracy of the contents herein and accepts no liability of any kind including without limitation warranties of merchantable quality, satisfactory quality, merchantability and fitness for a particular purpose on those arising by law, statute, usage of trade, course of dealing or otherwise. Matrikon shall not be liable for any losses or damages of any kind caused or alleged to be caused directly or indirectly from this manual.

LICENSE AGREEMENT

This document and the software described in this document are supplied under a license agreement and may only be used in accordance with the terms of that agreement. Matrikon reserves the right to make any improvements and/or changes to product specifications at any time without notice.

TRADEMARK INFORMATION

The following are either trademarks or registered trademarks of their respective organizations:

Matrikon and MatrikonOPC are trademarks or registered trademarks of Matrikon Inc.

OTHER

MatrikonOPC™ is a division of Matrikon™ Inc.

Table of Contents

Table of Tables

Introduction

All OPC communication is based on Microsoft COM (Component Object Model) technology. OPC uses DCOM (Distributed Component Object Model) technology for remote communication, so you must properly configure DCOM permissions to achieve successful communication between OPC components.

The included information will guide you through the process of setting DCOM to enable all communication. This is preferable for testing/diagnostic purposes.

Users often experience difficulties with OPC communication on Microsoft Windows XP SP2 and Windows 2003 SP1 due to advanced security settings. This document describes how to disable these security settings to allow OPC communication. This document also relates to Microsoft Windows SP3 and Microsoft Windows Server 2003 SP2.

Note: This guide shows you how to enable all DCOM permissions for OPC communications. It is up the user to disable unused DCOM settings to prevent unauthorized entry to their OPC server.

Required Software

This guide has been written and tested for all versions of:

- Microsoft Windows XP Pro
- Microsoft Windows Server 2003

Some settings, such as Data Execution Prevention (DEP) are relevant for only Windows XP SP2 and SP3, and Windows Server 2003 SP1, SP2, and R2.

Who Should Use This Guide

This guide is designed for users who are attempting to connect to an OPC server using DCOM and cannot establish connectivity.

Overview of Guide

This document uses icons to highlight valuable information. Remember these icons and what they mean, as they will assist you throughout the manual.

	This symbol denotes important information that must be acknowledged.
BOLD	Font displayed in this color and style indicates a hyperlink to the applicable/associated information within this document, or if applicable, any external sources.

The chapters in this document are structured as follows:

- **Introduction** – this introductory chapter.
- **DCOM Security Settings** – provides information about setting DCOM permissions to allow communication between DCOM objects.
- **Windows Firewall** – guides you through the steps needed to disable the firewall, if required.

- **Data Execution Prevention** – guides you through the steps needed to disable the DEP, if required.
- **Local Security Policy** – guides you through the steps needed to establish communication if you are using workgroups.
- **Limitations** – outlines connectivity limitations.

References

This document references information found within the following documents/sites:

- **www.matrikonopc.com**
- **www.opcsupport.com**
- **www.opsfoundation.org**

Document Terminology

Table 1 provides a list of definitions for terms throughout this document.

Term/Abbreviation	Description
DCOM	Distributed Component Object Model
DEP	Data Execution Prevention
ACL	Access Control List

Table 1 - Terms and Definitions

Contacting Support

The MatrikonOPC Customer Services department (**www.opcsupport.com**) is available 24 hours a day, seven days a week.

Contact MatrikonOPC Support using the information below, or send an email (**support@MatrikonOPC.com**).

For Monday to Friday **daytime support** requests, contact MatrikonOPC Support using the regional phone numbers provided in Table 2.

Region	Office Hours	Contact Information
North America UTC/GMT -7 hours (MST)	8:00 am-5:00 pm	**+1-877-OPC-4-ALL**
Europe /Africa * UTC/GMT +1 hours (CET)	9:00 am-5:00 pm	**+49-221-969-77-0** **(Request OPC Support)**
Australia/Asia * UTC/GMT +10 hours (AEST)	9:00 am-5:00 pm	**+61-2-4908-2198** **(Request OPC Support)**

* Toll-free regional numbers coming soon!

Table 2 - MatrikonOPC Support Regional Contact Information

For **after-hours support** in all regions, please use either of the following numbers. There is no extra charge from MatrikonOPC for calling their after-hours support numbers.

Region	Contact Information
All	+1-780-231-9480 +1-780-264-6714

Table 3 - After-Hours Support

DCOM Security Settings

OPC uses ActiveX COM and DCOM to communicate, so we must set the DCOM permissions to allow communication between DCOM objects.

1. Go to **Start** -> **Run** or use the **Windows Key**+**R** shortcut to launch the **Run** window.

2. Type in ***dcomcnfg*** and click OK.

3. In the **Component Services** window, navigate to **Console Root** -> **Component Services** -> **Computers** by clicking on the **+** icons to the left of the headings. Right-click on **My Computer** and select ***Properties***.

4. On the **My Computer Properties** window, ensure that the following settings are properly configured:
    a. On the **Default Properties** tab (Figure 1);
        i. The **Enable DCOM on this computer** option is checked
        ii. The **Default Authentication Level** is set to ***Connect***, and
        iii. The **Default Impersonation Level** is set to ***Identify***

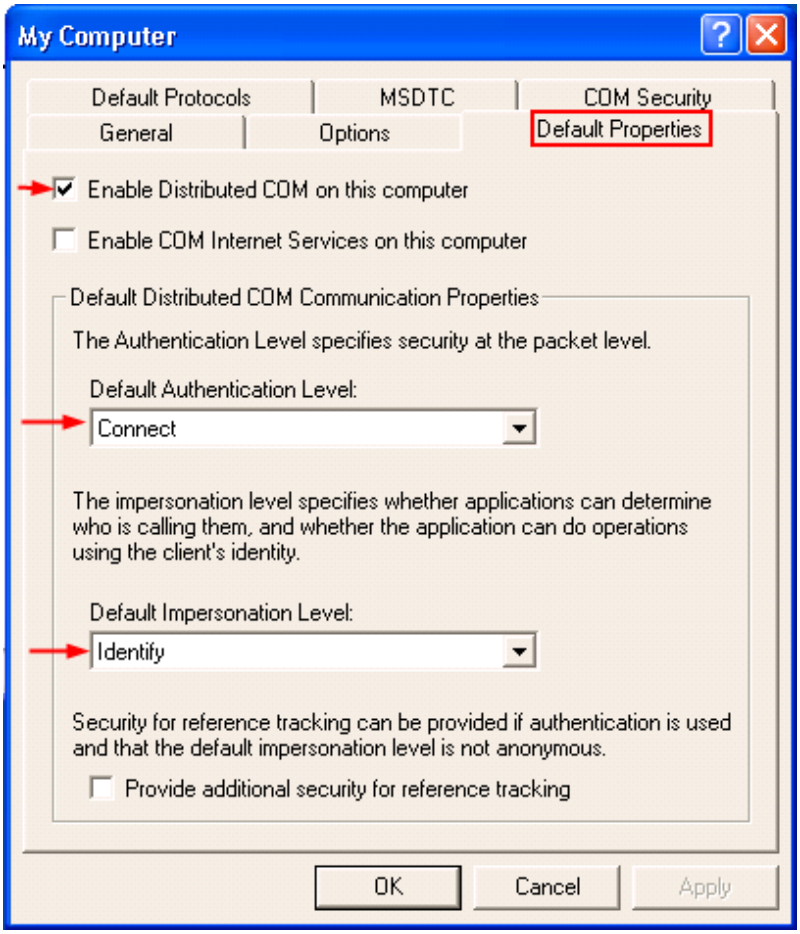


Figure 1 My Computer properties - Default Properties settings

b. On the **COM Security** tab (Figure 2);

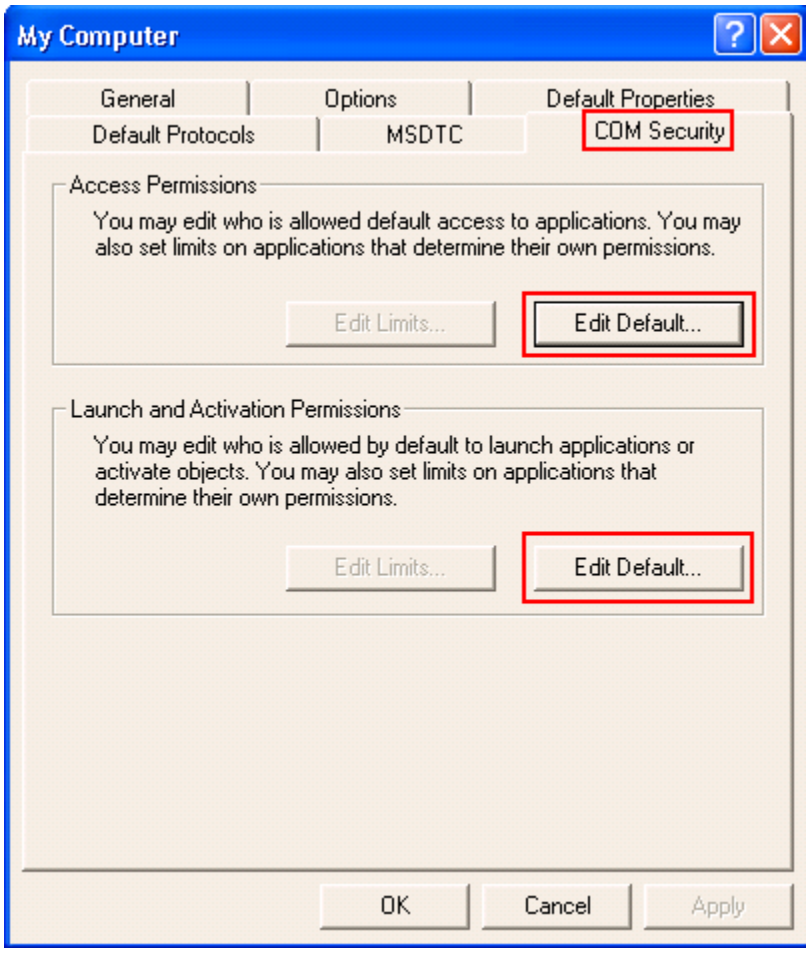


Figure 2 My Computer properties - COM Security settings

i. Under **Access Permissions** (Figure 3) click on the ***Edit Default*** button.
ii. Add the following. Do not remove any others that may already be listed there
    1. Anonymous Logon, this must be added in order for OPC Enumerator to function correctly.
    2. Everyone
    3. Interactive
    4. Network
    5. System
iii. Ensure that both **Local** and **Remote** Access are ***Allowed***
iv. Click on **OK**

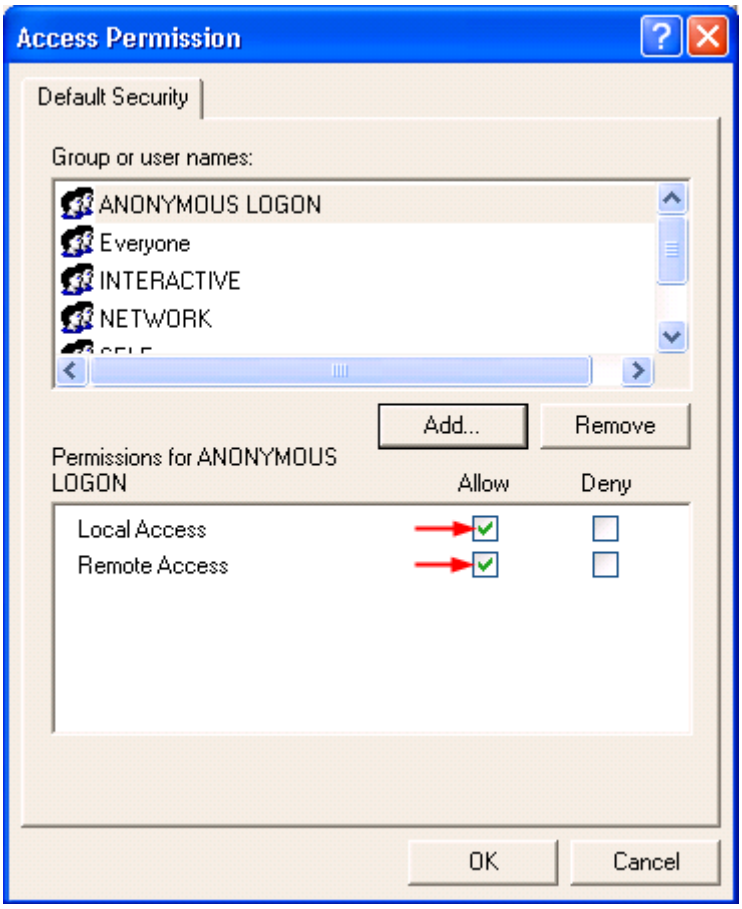


Figure 3 Access Permissions dialogue

v. Under **Launch and Activation Permissions** (Figure 4) click on the ***Edit Default*** button
vi. Add the following. Do not remove any others that may already be listed there
    1. Anonymous Logon
    2. Everyone
    3. Interactive
    4. Network
    5. System
vii. Ensure that **Local** and **Remote** Launch and Activation are ***Allowed***
viii. Click on **OK**

c. The **Edit Limits** (Figure 2) option in this tab applies machine-wide settings for **Access** and **Launch** permissions. This is an additional layer of security added in Service Pack 2 for Windows XP and Service Pack 1 for Windows 2003. These settings are the same as the DCOM options in the Local Security Policy, but are recorded in different Registry keys. Due to the fact that Windows applies Local Security Policies with a higher priority than the Registry keys applied by these settings, when the Local Security Policy Options for these configuration items are set, the **Edit Limits** buttons will be greyed out or *inactive*.
When configuring the DCOM settings for your computer, if the **Edit Limits** buttons are *active*, do not make changes here. The procedure for configuring the Local Security Policy Options will negate these changes, and will be covered later in this document.

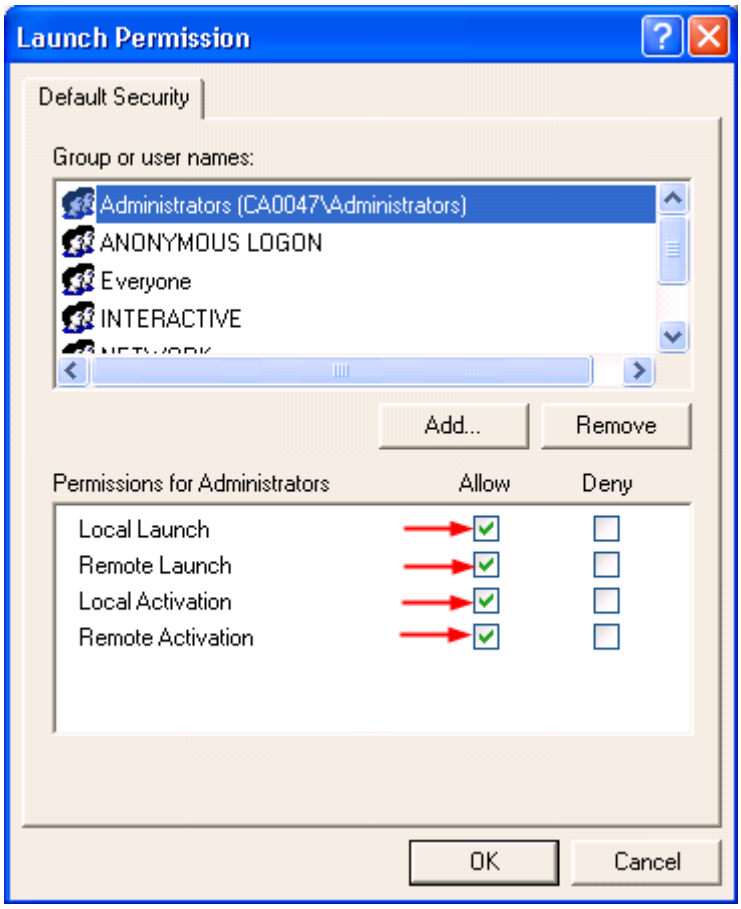


Figure 4 Launch and Activation permissions

5. The DCOM settings for each OPC Server object must now be individually configured. This serves two (2) purposes;
    a. It removes dependence on the Default settings for each server, and
    b. It allows for permissions on each Server object to be restricted to only those who require it.
6. Under **My Computer**, open the folder labelled ***DCOM Config***.

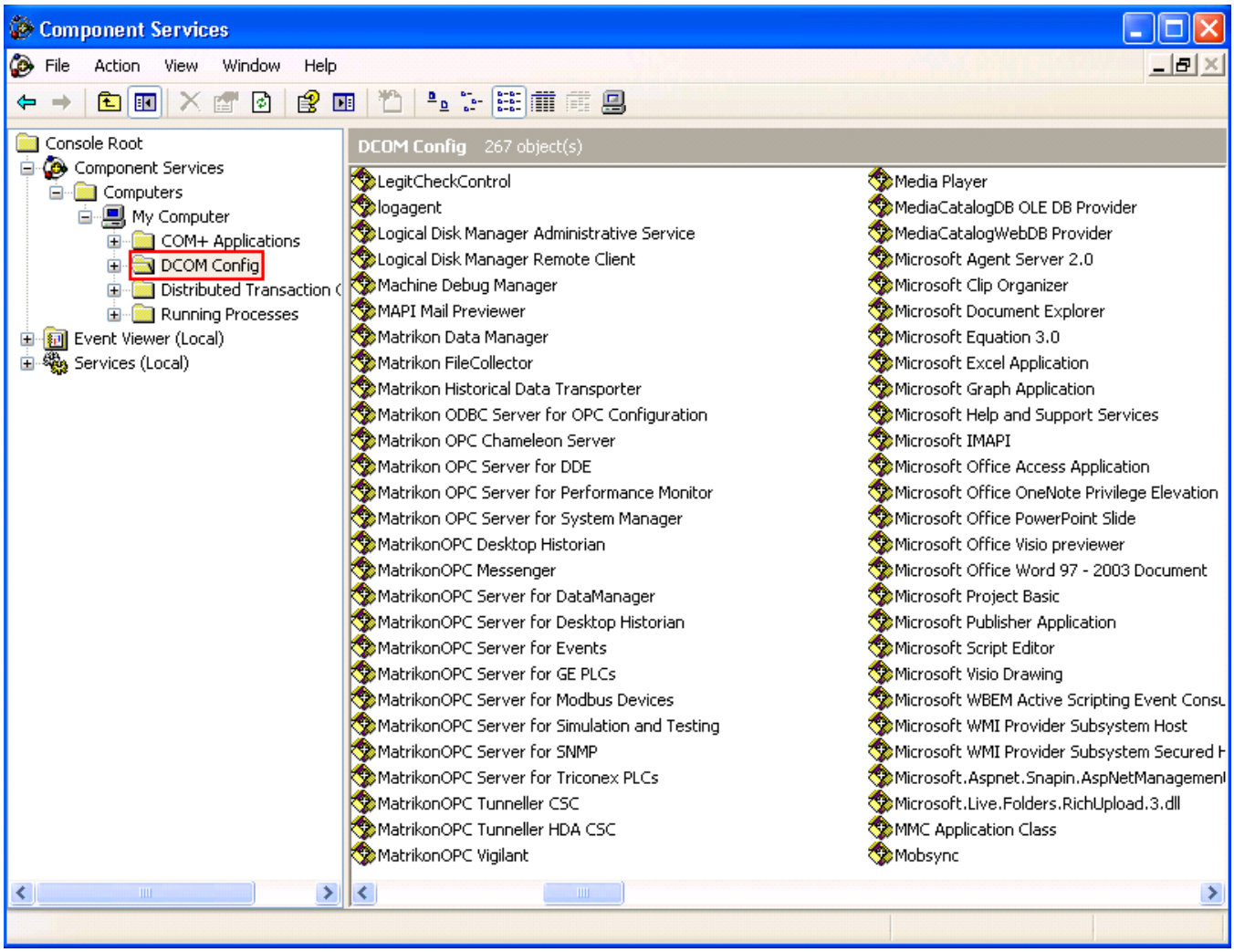


Figure 5 DCOM Objects list

7. To edit the settings for each OPC Server, browse to the OPC Server, right-click on it, and select **Properties**.

    a. On the **General** tab (Figure 6), set the **Authentication Level** to ***Connect***.

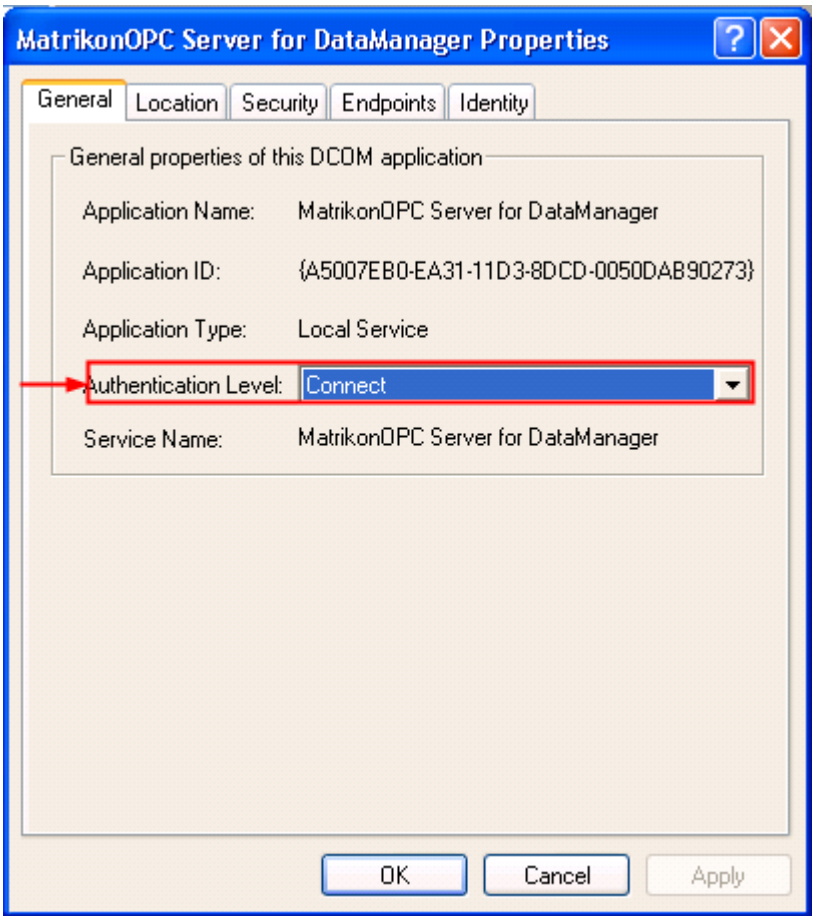


Figure 6 DCOM Settings - General tab

b. On the **Security** tab (Figure 7);
   i. Under **Launch and Activation Permissions**, select the **Customize** radio button. Then click on **Edit**.

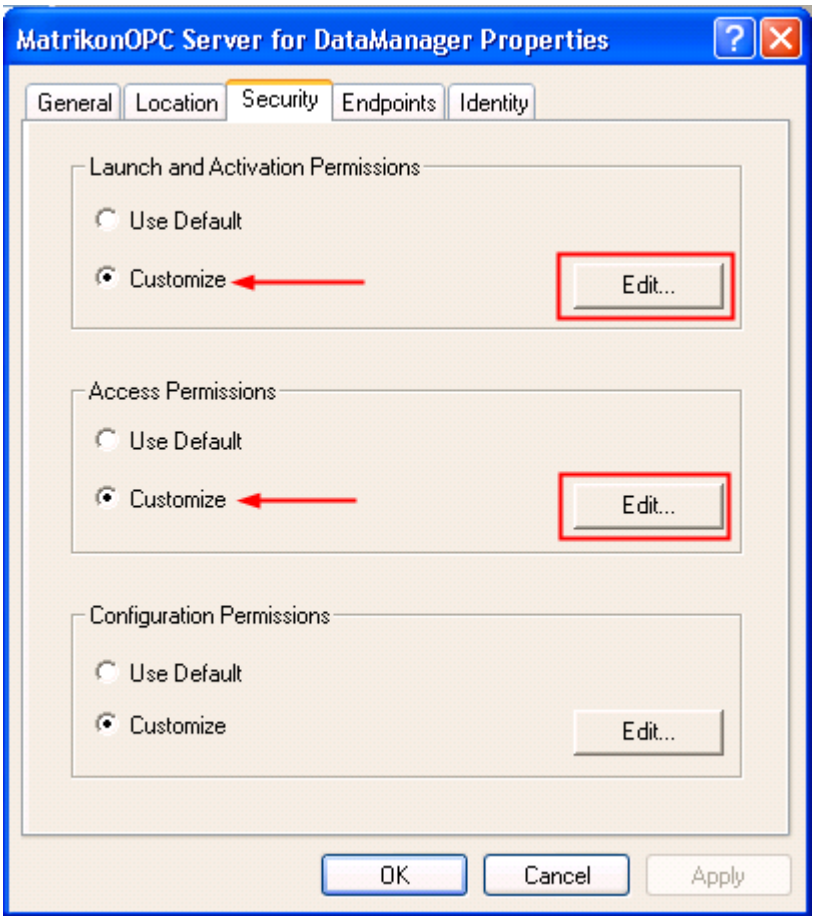


Figure 7 DCOM Settings - Security tab

ii. Add the following users;
    1. Everyone
    2. Interactive
    3. Network, and
    4. System

iii. Ensure that all Users have **Local** and **Remote**, **Launch** and **Activation** permissions *Allowed* selected. Then click **OK**.

iv. Under **Access Permissions** select the **Customize** radio button. Then click **Edit**.

v. Add the following users;
    1. Everyone
    2. Interactive
    3. Network, and
    4. System

vi. Ensure that all Users have **Local** and **Remote**, **Access** permissions *Allowed* selected. Then click **OK**.

c. On the **Endpoints** tab (Figure 8), ensure that *Connection oriented-TCP/IP* is entered in the list

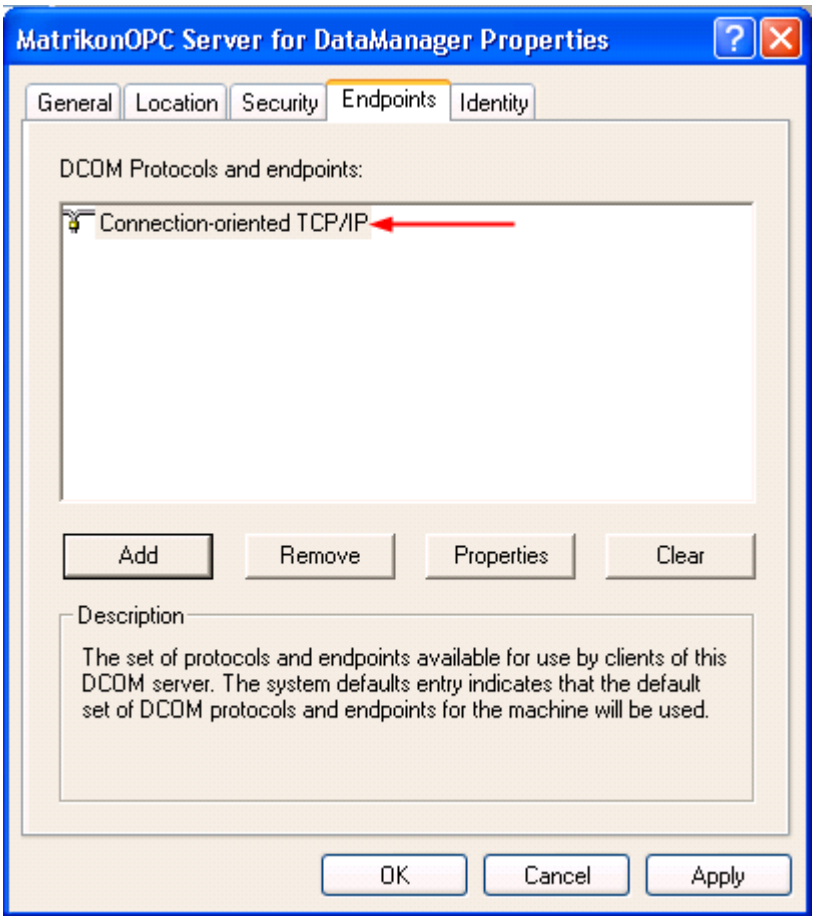


Figure 8 DCOM Settings - Endpoints tab

d. On the **Identity** tab (Figure 9), ensure that your server is running as *This user,* whether the object is registered as a Service or as an Application. If it is running as a service, the **System account** can also be used. The recommended setting for this is to run as a service using the System Account identity. It is highly recommended that the Launching User identity not be used. Click **OK** to return to the **Component Services** window.

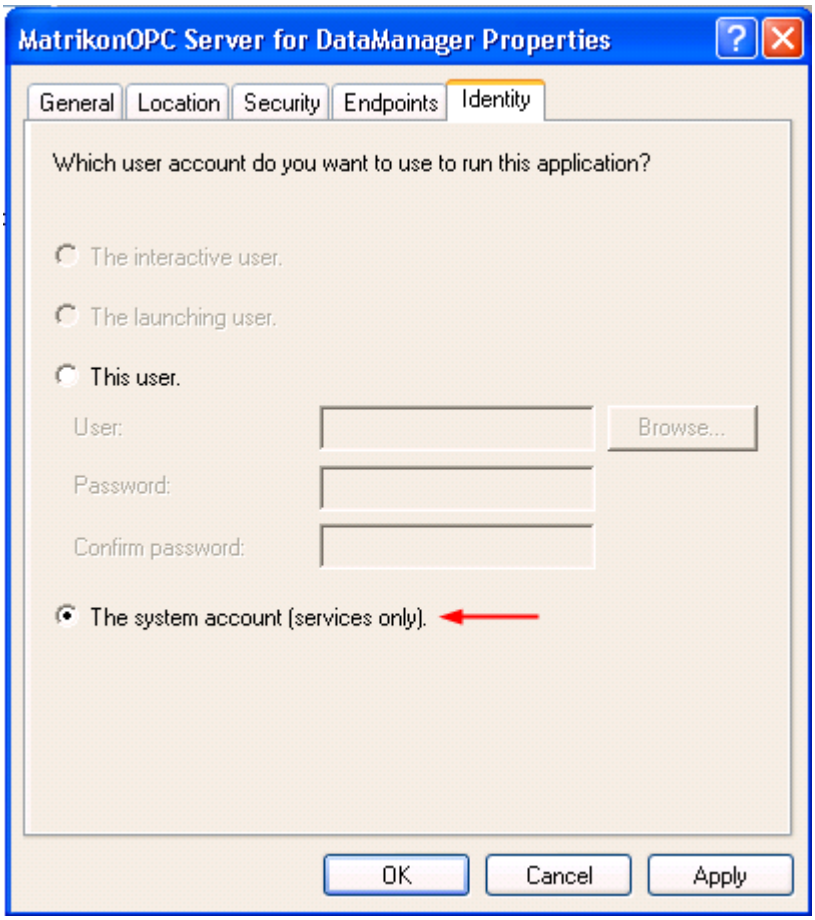


Figure 9 DCOM Settings - Identity tab

Additional Security Notes

By setting the Identity to "Interactive User" it is necessary to remain logged on at this computer in order for the application to run. This may represent a contradiction of your Company IT Security Policy. If this software must be run as an application, it may be more effective to run as *This User* and provide credentials for the application to use.

In order for the server objects to be properly discovered by the clients, the OPC Server List Utility, OPC Enumerator, must also be properly configured for DCOM. This utility is a COM server and must allow connection and access by the clients as well.

Windows Firewall

For Service Pack 2 to Windows XP and Service Pack 1 for Windows 2003, the Windows Firewall was turned on by default. This software firewall will prevent DCOM communication by blocking the remote calls that DCOM requires for such functions as DNS name resolution, function calls and callbacks, to name a few. Exceptions can be made in the firewall, either by application or by port number. This process is described elsewhere, for example in the Windows Help files. The issue is that DCOM requires such a wide range of ports be opened that there are serious gaps left in the security of the system thus configured.

It is more effective to turn the firewall off, if permitted by your company IT policy. If not permitted, contact your IT department and request permission to temporarily turn it off in order troubleshoot the system. To turn off the Windows Firewall, follow this procedure;

1. Navigate to **Windows Control Panel**
2. Double click on the **Windows Firewall** icon.
3. Set the Windows Firewall to *OFF*, and click **OK**.

Data Execution Prevention

Data Execution Prevention (DEP) is a set of hardware and software technologies that perform additional checks on memory to help prevent malicious code from running on a system. In Microsoft Windows XP Service Pack 2 (SP2), Microsoft Windows Server 2003 SP1 and Microsoft Windows XP Tablet PC Edition 2005, DEP is enforced by hardware and by software.
DEP will also prevent many installations from running, and has been known to cause other software issues. Most MatrikonOPC software released since late 2006 will detect the DEP setting and, if turned on, terminate the installation process.

Most MatrikonOPC Software released since August 2009 no longer requires DEP to be turned off. Please verify this by reading the release notes and user manual for each software installed.

If the software has been installed with DEP turned on, the following steps must be performed;

1. Turn DEP *OFF*
2. Restart the Operating System
3. Uninstall the OPC software
4. Re-install the OPC software

To turn DEP *OFF*, perform the following steps:

1. From your Start menu, right-click on **My Computer** and select **Properties**.
2. On to the **Advanced** tab (Figure 10), under **Performance**, click the **Settings** button.

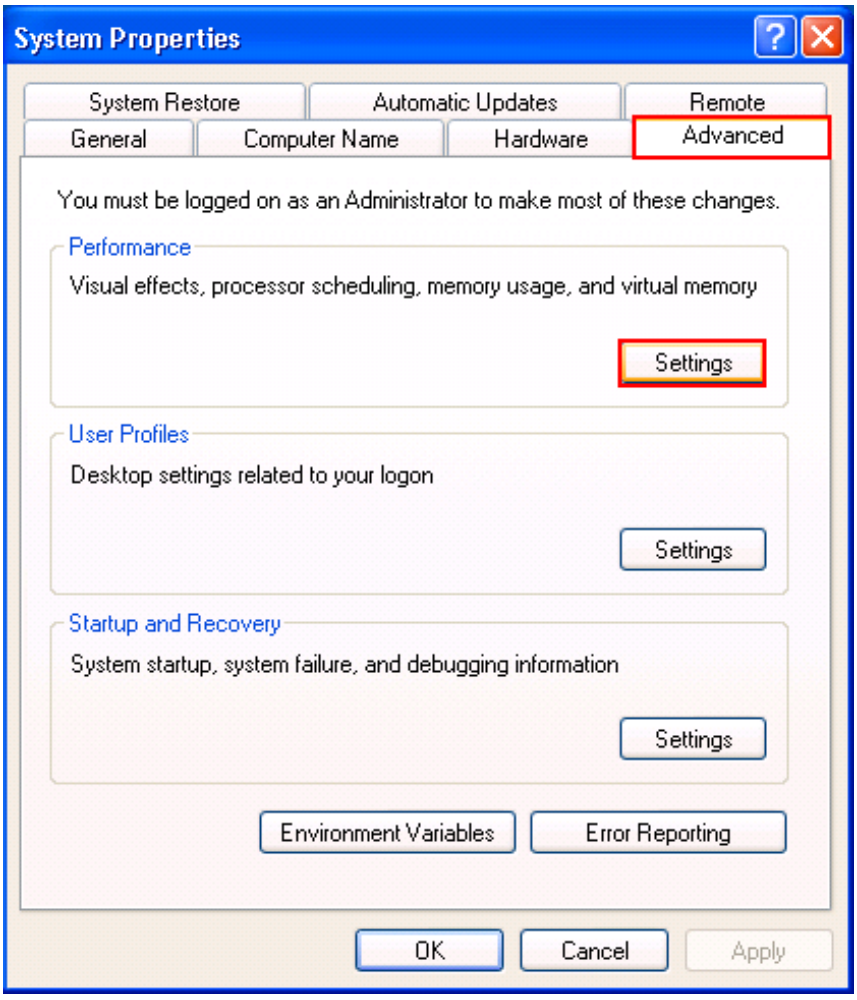


Figure 10 System properties dialogue

3. On the Performance Options tab (Figure 11), select the **Turn on DEP for essential Windows programs and services only** option. This is the setting we refer to as *OFF*.

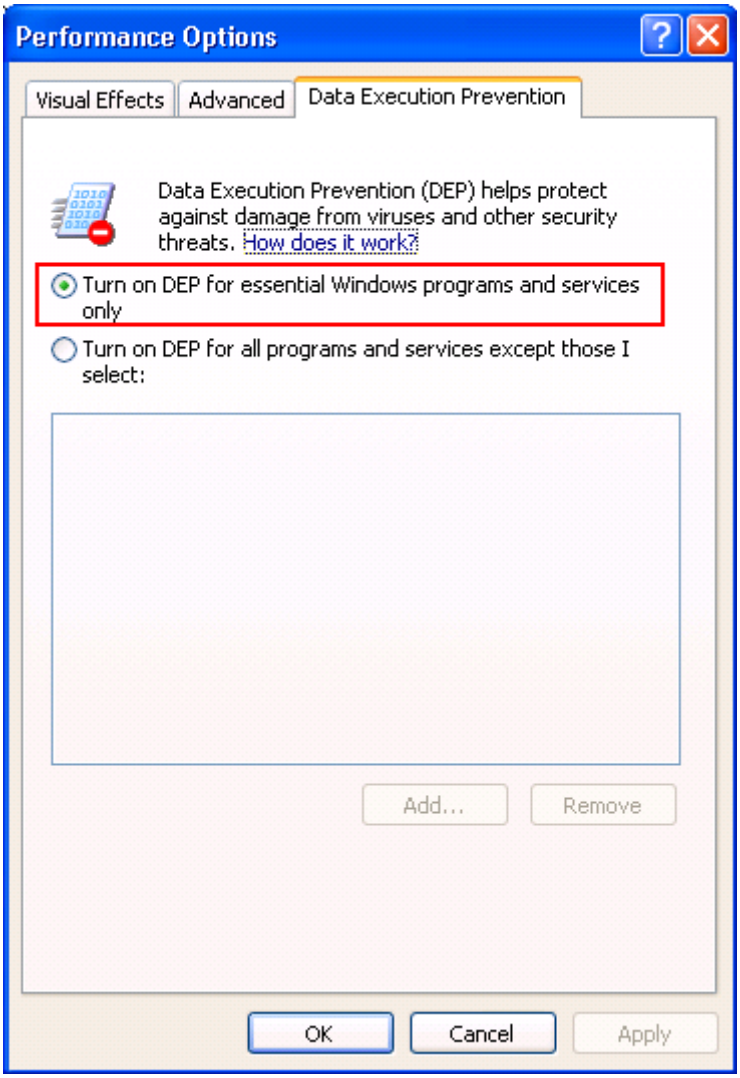


Figure 11 Performance Options dialogue

4. Click **OK**. If you changed the setting, it will be necessary to restart the operating system.

Local Security Policy

If you are using workgroups instead of domains the following steps may need to be taken in order to establish communication. Please note that these changes may compromise the security of your system – speak with your network administrator if you have any concerns.

1. Navigate to **Start**->**Settings**->**Control Panel**->**Administrative Tools**->**Local Security Policy**.
2. Navigate to **Security Settings**->**Local Policies**->**Security Options** (Figure 12).
3. Right-click on **DCOM: Machine Access Restrictions...** and select **Properties** or; double-click on this option. Either method will open the **Properties** dialogue.

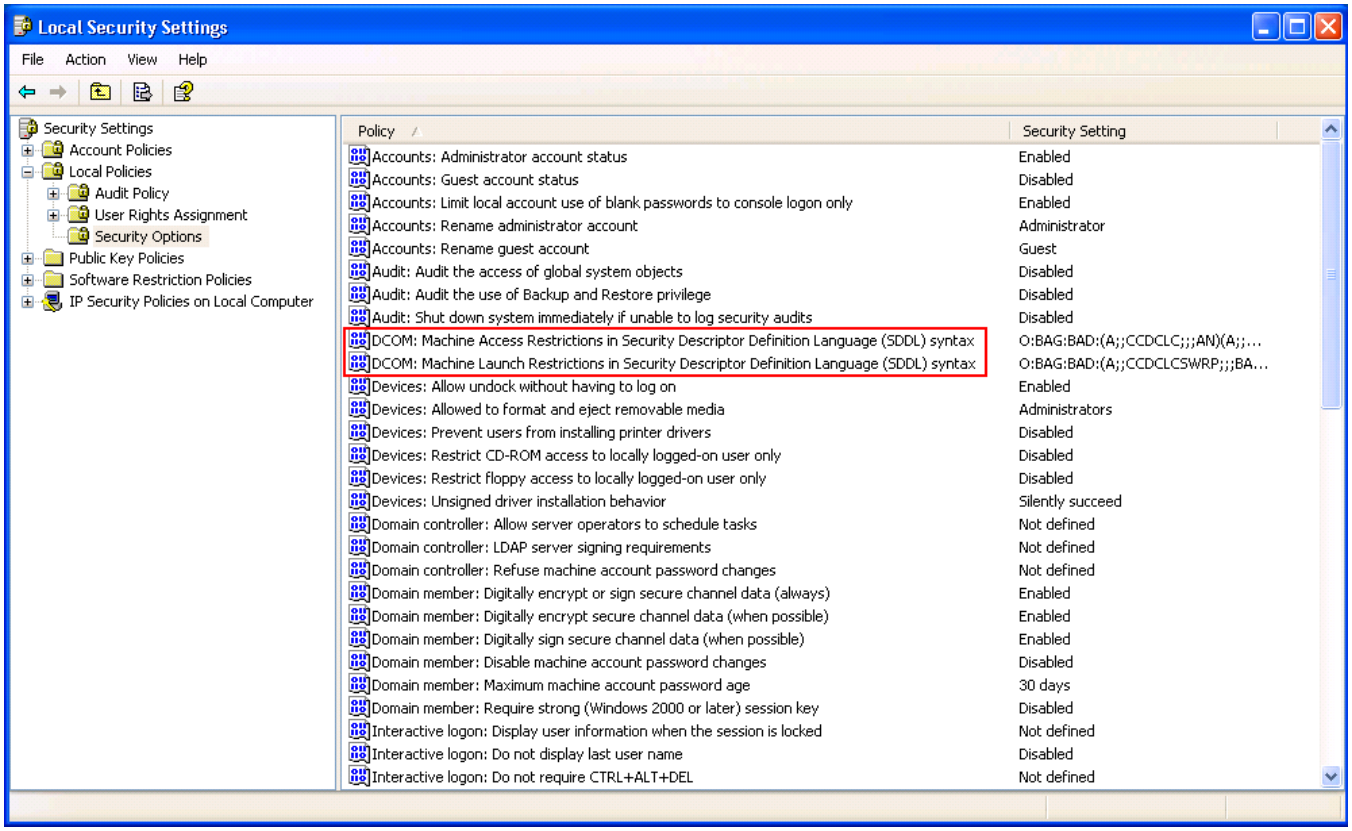


Figure 12 Local Security Settings dialogue

4. Click on the **Edit Security** button.

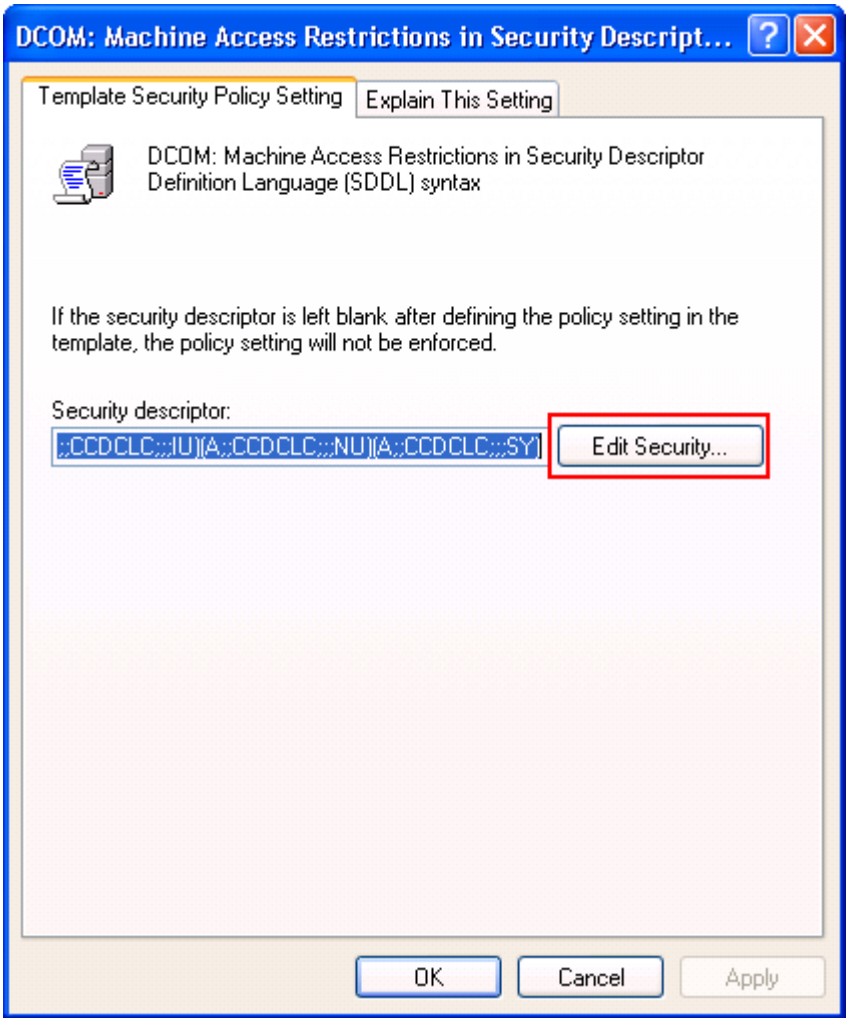


Figure 13 Machine Access Restrictions dialogue

a. Ensure that the following Users / Groups are added and that all have Local and Remote Access allowed (this is the same as the Access permission configuration in the Default DCOM settings);
    i. Anonymous Logon
    ii. Everyone
    iii. Interactive
    iv. Network, and
    v. System
b. Click OK to return to the main security policy window.

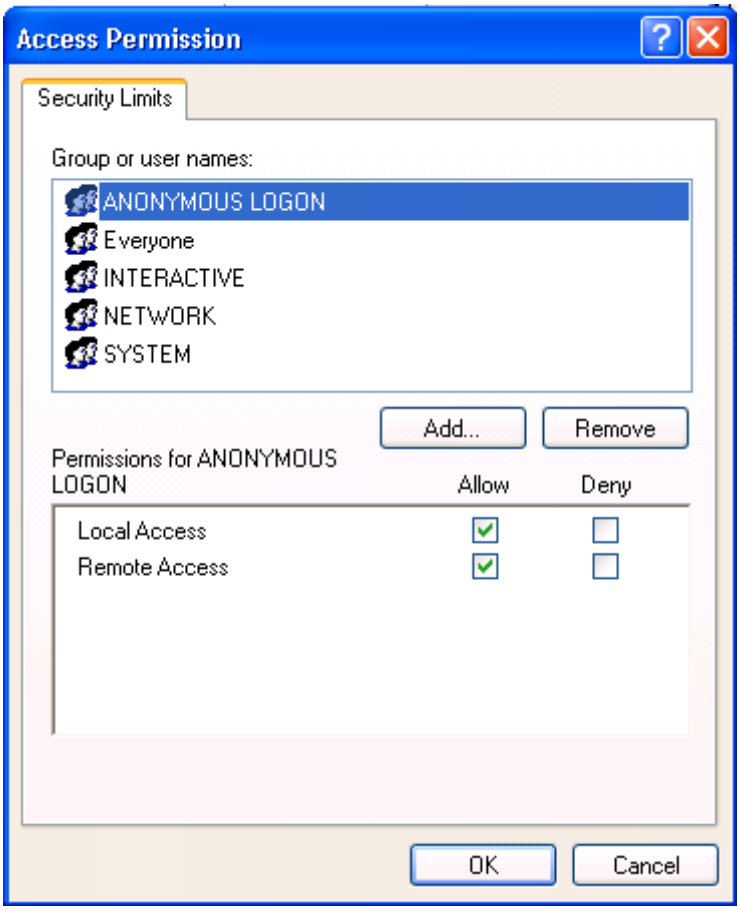


Figure 14 Access Permissions dialogue

5. Repeat this process for the DCOM: Machine Launch restrictions settings
6. Return to the Local Security Policy Options and select the **Network Access: Let Everyone permissions apply to anonymous users**

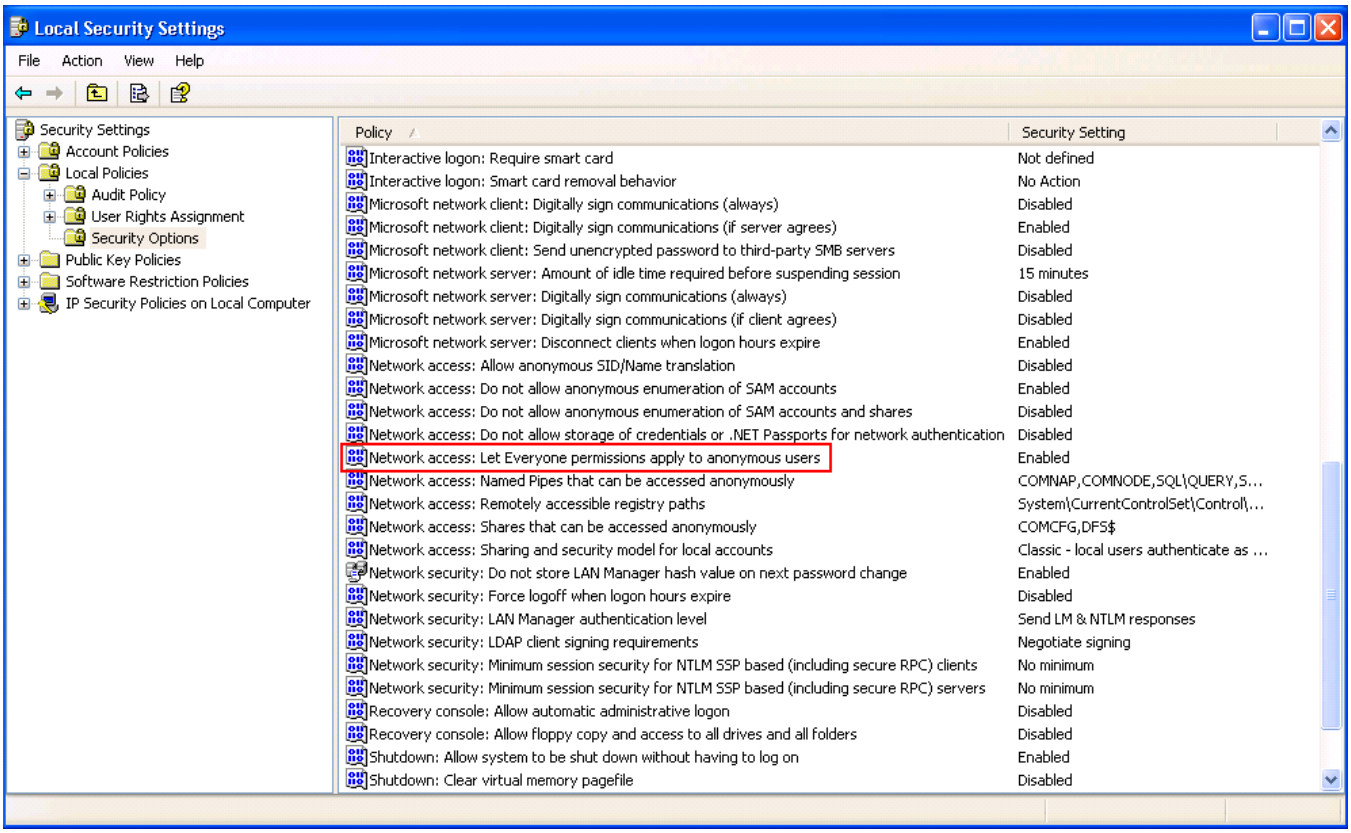


Figure 15 Local Security Settings - Network Access

7. Enable this option by double-clicking on the setting to open the dialogue in (Figure 13), and selecting **Enable**.

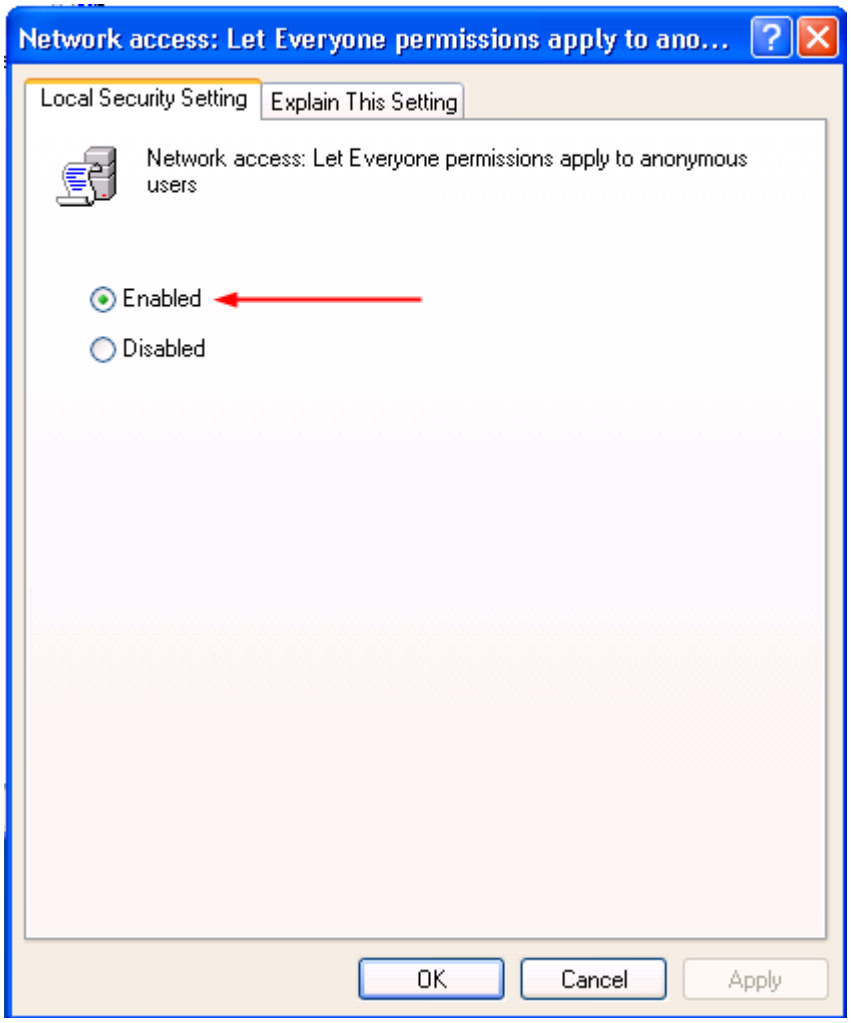


Figure 16 Network Access – Everyone permissions

8. Return to the Local Security Policy Options and select the **Network Access: Sharing and security model for local users**

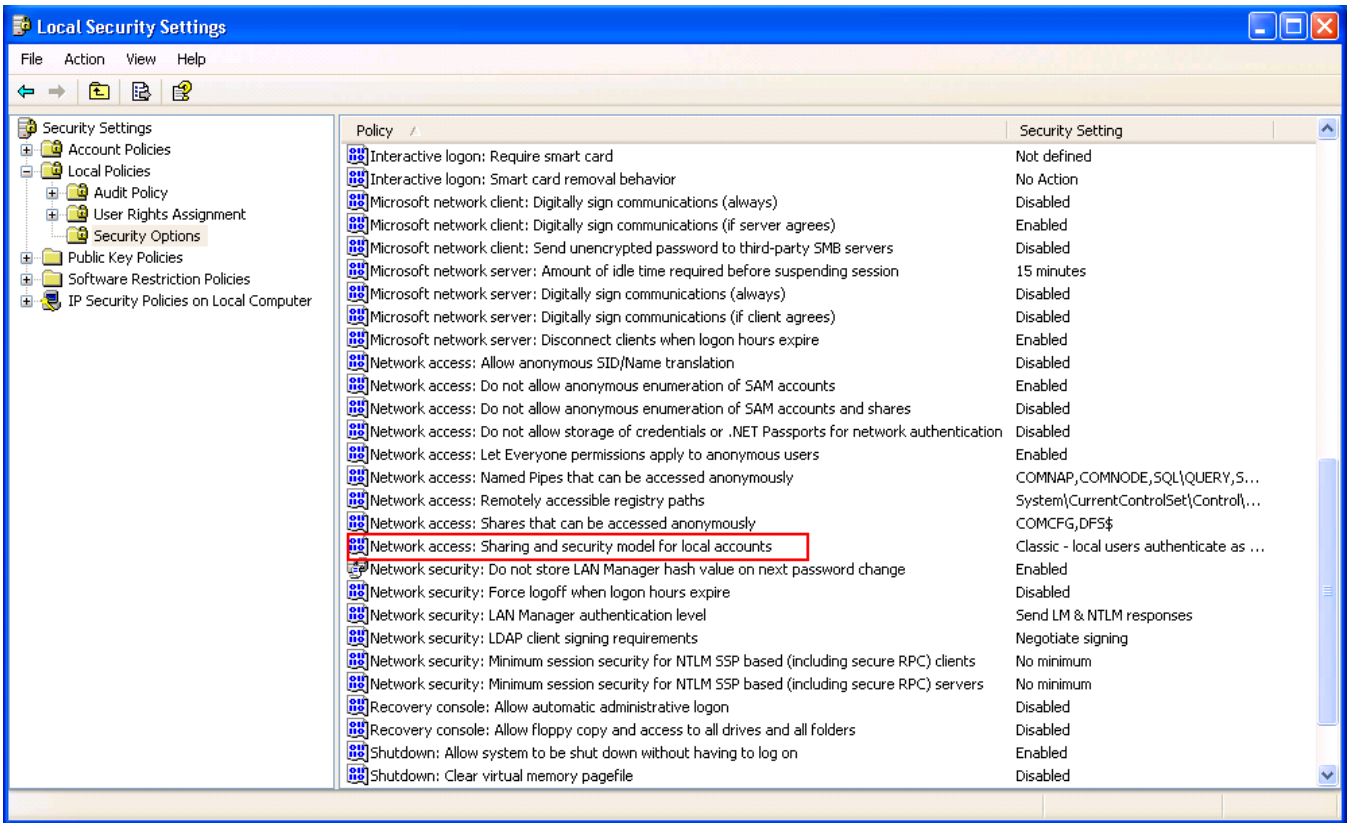


Figure 17 Local Security Settings – Network access: Sharing and Security model

9. Select the **Classic** option by double-clicking the setting to open the dialogue at (Figure 17), and select from the drop down menu.

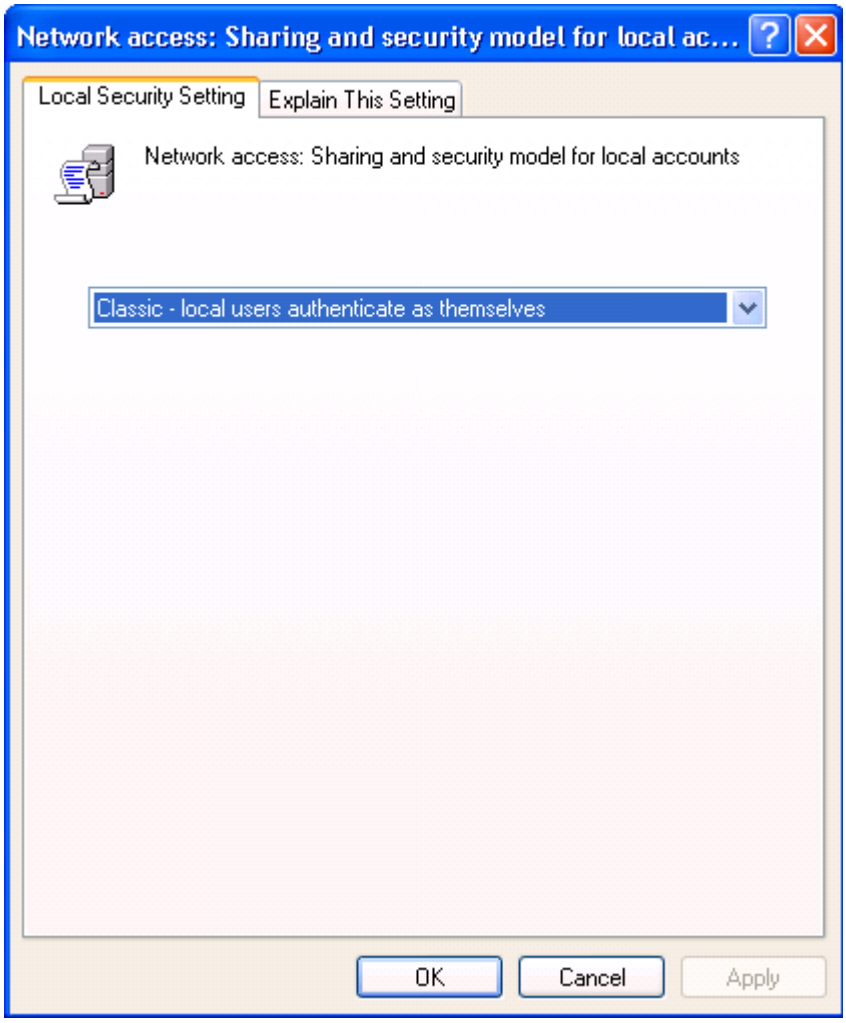


Figure 18 Network access: Sharing and security model dialogue

10. Return to the Local Security Policy settings and select **User Rights Assignment** from the **Local Policies** group. Double-click on the **Access this computer from the network** to open the dialog for this setting.

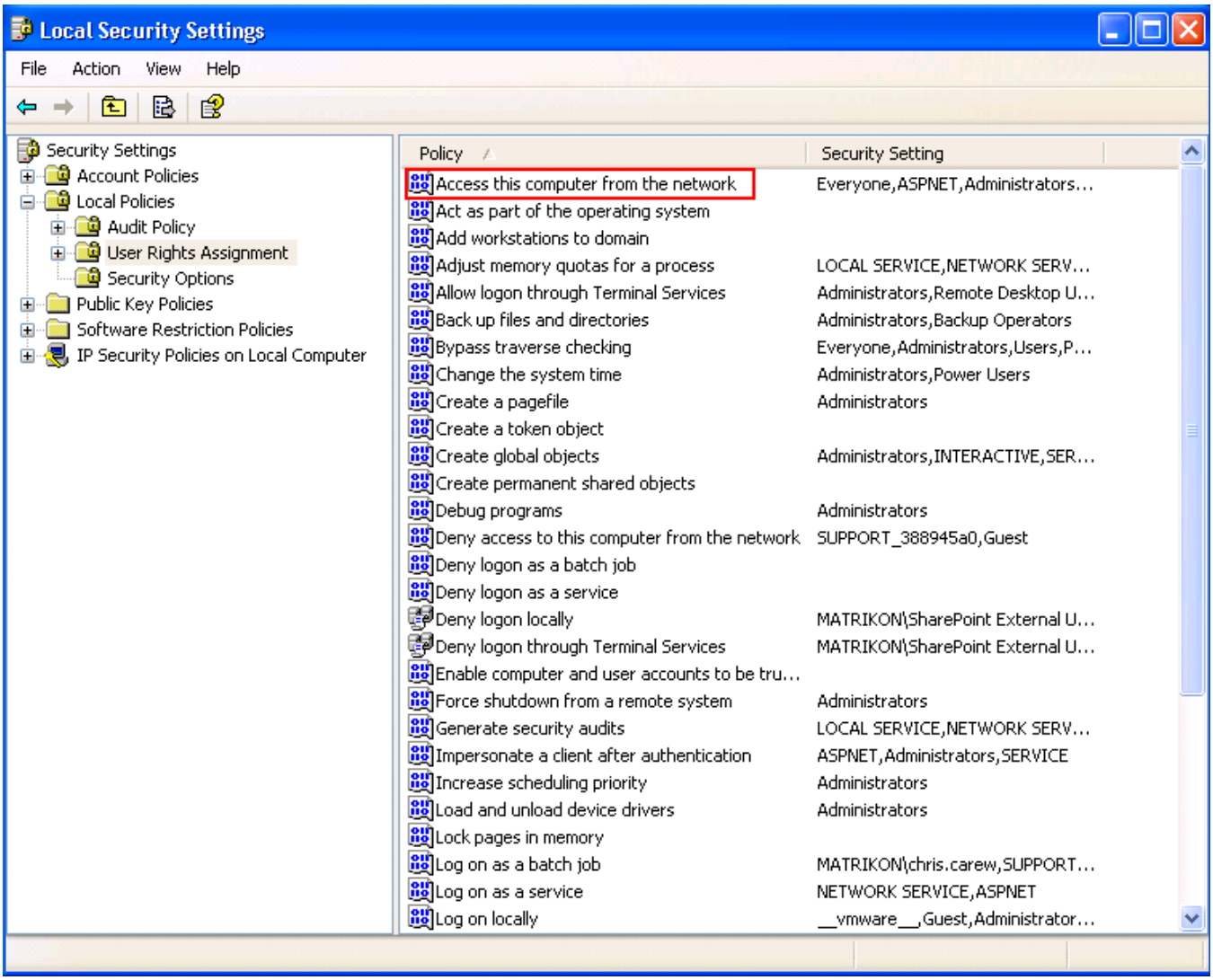


Figure 19 Local Security Settings – User Rights Assignment

11. Ensure that all Users are added to this setting to allow access from the network.

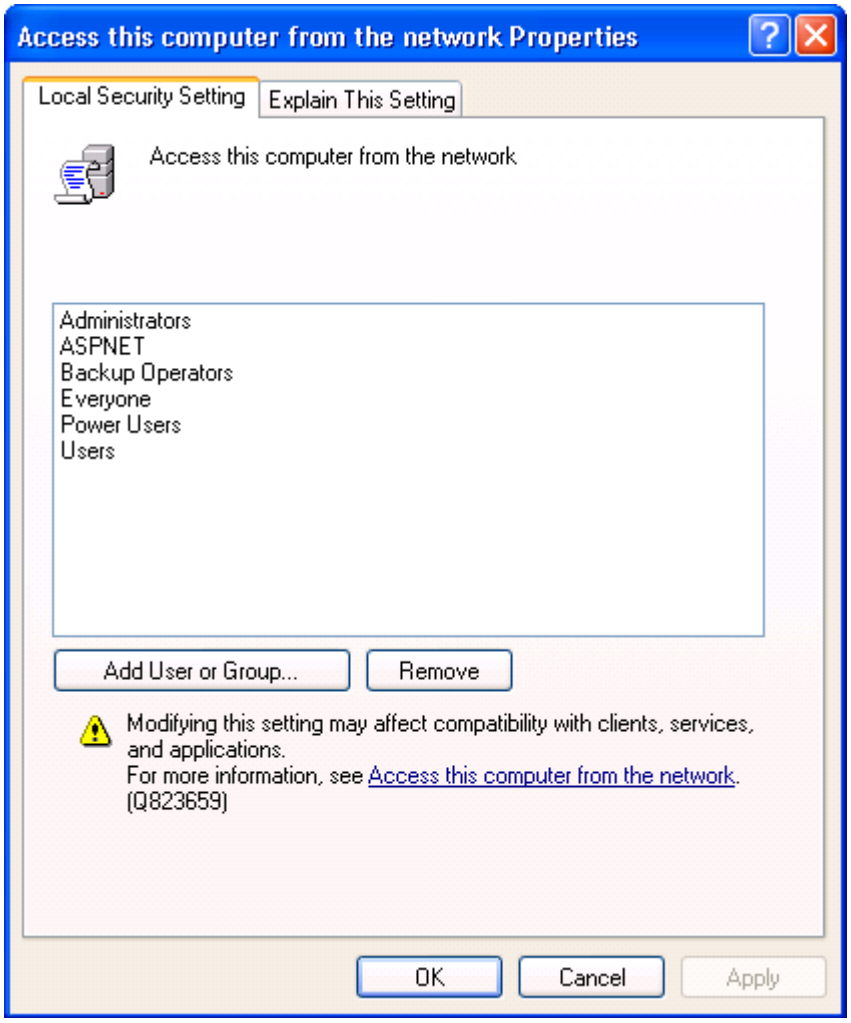


Figure 20 Network access properties dialogue

12. Your DCOM is now setup to accept all incoming connections.

Notes:

- These settings will allow full access to your system. This allows for easy communication in most cases. It also has set the security on your system to its lowest state. From this state you can narrow down the security settings so that only those who require access to your system are permitted. This is most easily accomplished using Groups rather than individual users.

Limitations

DCOM was developed to function in a specific environment where the following conditions applied;

1. All machines and users belonged to the same domain
2. There were no firewalls enabled on any machines or network devices
3. All communication media were highly reliable
4. There were no bandwidth restrictions

All of these were typical of a LAN setup in an average office environment. However, this bears little resemblance to the process control networks of today. Multiple domains, IT policies that dictate that the Windows Firewall be enabled on all machines, geographically dispersed sources of data and a multitude of other factors all make OPC communication based on DCOM extremely complicated to configure and still maintain security.

Tunnelling technology can provide successful DCOM communications across firewalls or domains/workgroups. Using a single TCP port to the remote computer, issues involving workgroups, domains and firewalls no longer hamper OPC communication. This allows you to establish OPC communication without sacrificing security.

The MatrikonOPC Tunneller is one of our most popular products because of it's ease of use, automatic reconnection system and time savings in implementation that it offers. Contact your Account Manager or visit our website at **www.matrikonopc.com** for more information on this, and other, MatrikonOPC solutions.